Serial Number 09/893,465

REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Rejection of Claims 1-4, 6, 11, and 13-17 Under 35 USC §102(b) in view of U.S. Patent No. 6,902,202 (Veil)

This rejection is respectfully traversed on the grounds that the Veil patent neither discloses nor suggests using a **smartcard**, as opposed to a security co-processor, to perform all digital signing operations that require access to a private key. In the system of Veil, the security co-processor 122 or "file signing tool" **retrieves the private key** from the smart card before performing a signing operation using the key.

The security co-processor 122 of Veil is clearly not, as alleged by the Examiner, on or part of the smart card. Instead, it is a separate device with an interface for communicating with the smart card. This is exactly contrary to the claimed invention, which seeks to protect the private key by keeping it on the smartcard and having the smartcard perform all operations that might compromise the key. Retrieval of the private key is precisely the type of exposure that the claimed invention seeks to avoid.

A side-by-side comparison reveals the difference:

Claimed	Veil
file signing tool accesses smartcard, sends data to smart card;	file signing tool (security co-processor 122) retrieves key from smart card;
the smartcard performs all digital signing operations that require access to a private key;	***the file signing tool performs all digital signing operations that require access to a private key.***
the results of the operations requiring access to a private key are sent back to the file signing tool so that the file can be signed	

According to the claimed invention, the private key never leaves the smartcard, and the file signing tool does not have access to the key. Instead, the file signing tool merely supplies data to the smartcard, which carries out any operations on the data that involve the key, and then sends back the results of the operations to the file signing tool for completion of the signing operation. This permits use of a file signing tool that may not be completely trustworthy without compromising private keys on the smartcard.

The Veil patent does recognize the vulnerability of the private key, but seeks to protect the private key through the use of PIN protection of the security co-processor. Unfortunately, in real life, PINs can be stolen or, even worse, the employee entrusted with the PIN might be corrupt. None of this bothers Veil, as is made clear from col. 11, lines 28-35:

> *Thus, in operation, the system in accordance with the present invention. . .reads from the smart card the account number, the digital certificate and, optionally, the private-key into the security co-processor (122), and then it prompts the smart card owner to enter the PIN via the trusted input device (130).*

In contrast to the claimed invention, Veil trusts the input device, and therefore believes the security co-processor to be secure enough to handle the private key. As a result, Veil neither discloses nor suggests having the smart card itself, as opposed to an external co-processor, perform operations involving the private key. While the private key is "optional" to the extent that it may be omitted entirely, if the private key is used, it is transferred to the security co-processor, which is part of a "secure computing environment" (col. 11, line 39). This is fundamentally different from and contrary to the claimed invention.

In the rejection, the Examiner paraphrases the claim language by stating that:

> *Veil teaches a smartcard having stored thereon a private key (Veil, column 11, lines 23-28, private key), a file signing tool arranged to receive a file to be signed (Veil, column 11, lines 1-11, data is captured and signed), to access the smartcard (Veil, column 11, lines 45-52), and to download signed files to the terminal (Veil, column 11, line 66 - column 12, line 3).*

This comparison by the Examiner of the claimed invention and Veil does not include an accurate statement of what is claimed. Instead, it ignores the language specifically included in claim 1,

"*wherein* ***the smartcard includes*** *an embedded secure processor programmed to perform all* ***digital signing operations that require access to the private key.***" Veil clearly does not suggest this positively recited feature of the invention, which is extensively discussed in the original specification. As explained in lines 15-17 on page 5 of the original specification, a potential weakness of file signing tools of the type disclosed by Veil "*lies in protection of the private key used to sign the files.*" Therefore, according to pages 5-6 of the original specification:

> *. . . When a digital signature is required, the PIN is entered and verified, and the private key is decrypted and accessed by a computing device which performs the computations necessary to generate the digital signature. As a result, the private key is vulnerable to duplication during the signing procedure.*

This is the problem that is solved by having the smartcard itself perform all operations that require access to the private key. It is a problem to which the file signing tool of Veil is clearly vulnerable. If the legitimate holder of the PIN described in the Veil patent is not trustworthy, or if the PIN has been stolen, the private key of Veil can easily be duplicated because access to the private key is permitted via the PIN that unlocks the smartcard.

As pointed out in the previous response, the Veil patent mentions the possibility of having the smartcard performing all security functions. However, Veil dismisses the possibility on grounds of cost and practicality (col. 1, line 66 to col. 2, line 7), and instead specifically *teaches away* from the approach taken by the claimed invention by teaching the addition of a security co-processor that retrieves the private key from the smartcard. **Whereas the claimed invention seeks to preclude access to the private key by any external processor, Veil specifically teaches a security co-processor designed to perform all processing operations, including operations involving the private key. This security co-processor of Veil is NOT on the smartcard itself, whereas claimed 1 specifically calls for having the smartcard itself perform all operations involving the private key.**

Accordingly, it is respectfully submitted that the new rejection of claims 1-4, 6, 11, and 13-17 under 35 USC §102(b) in view of the Veil patent is improper and withdrawal of the rejection is respectfully requested.

2. Rejection of Claims 5 and 17 Under 35 USC §103(a) in view of U.S. Patent Nos. 6,092,202 (Veil) and 5,659,616 (Sudia)

This rejection is respectfully traversed on the grounds that the Sudia patent, like the Veil patent, neither discloses nor suggests the combination of a file signing method in which a file signing tool is arranged to perform private key file signing operations ***without accessing the private key***, as claimed, by accessing a smartcard that performs all digital signing operations that require access to a private key. Instead, Sudia teaches having the smartcard sign the file.

The methods of Veil, Sudia, and the claimed invention may be summarized as follows:

	Sudia	Veil	Claimed
File Signing Tool?	No	Yes	Yes
Tool Retrieves Key?	N/A	Yes	No
Comments	Teaches having smartcard perform all file signing operations	Teaches away from smart card performing file signing operations on grounds of "cost and practicality"	Offers convenience of a separate file signing tool with the security of smartcard key protection

It is true that the system of Sudia discloses use of a smartcard to authenticate a transaction by providing a private key. However, the Applicant has not claimed to have invented the concept of signing files by using a private key, and authenticating the files by means of a certificate that includes the corresponding public key. Instead, the invention is directed to the use of file signing tool that enables use of private key encryption to authenticate files being downloaded to a terminal, such as terminal update programs. Sudia does not teach such a tool, while Veil teaches that if a file signing tool is used to sign files by means of a private key, the file signing tool should retrieve the private key from a smartcard.

In Sudia, the smartcard itself, *rather than a file signing tool*, signs the "transaction." There is no suggestion of a file signing tool of the type claimed. Use of the smartcard to sign "transactions" is appropriate in the context of Sudia, since transactions are files that contain

limited information, such as amounts. In contrast, the claimed invention involves downloading of files of arbitrary size, such as operating program or database updates, to a transaction terminal rather than just signing of transactions. Since Sudia does not teach any sort of file signing tool, it could not have suggested modification of the file signing tool of Veil in the manner claimed. Instead, Veil clearly ***teaches away*** from applying from the concept disclosed by Sudia, namely use of a smartcard for the entire file signing operation, because a smartcard cannot perform the extensive calculations that might be necessary to sign a file of arbitrary size.

In summary, while it is true that Sudia teaches use of a smartcard to protect a private key, the claimed invention is not merely to protect a private key using a smartcard, but rather to provide a tool that permits a smartcard-protected private key to be used to authenticate files being downloaded to a terminal while still protecting the private key. Veil does teach a file signing tool, but teaches away from combining it with a smartcard in the manner claimed, the Veil patent instead teaching that the file signing tool should retrieve the private key from the card in a "secure" environment. Because the Veil and Sudia patents do not disclose or suggest all elements recited in the claims corresponding to original independent claims and 1 and 11, withdrawal of the rejection under 35 USC §102(b) is respectfully requested.

In addition, it is again respectfully noted that Sudia and Veil patents fail to even disclose the **terminal-installed** certificate recited in claims 5 and 17, which is for use by the terminal in **authenticating the signer certificate**. According to item 17 on page 6 of the Official Action, this feature is disclosed in col. 13, lines 30-41 of the Veil patent. However, the cited passage actually refers to a cache of pre-verified *signer* certificates. In other words, the system of Veil stores pre-verified copies of the signer certificate, so that it only has to authenticate the signer's certificate one time, after which it merely checks to see if the received signer certificate is the same as a pre-verified one. **This is not the same as authenticating the signer certificates themselves to protect against loading of attempts to download inauthentic certificates.**

Accordingly, withdrawal of the rejection of claims 5 and 17 under 35 USC §103(a) is respectfully requested.

3. Rejection of Claim 10 Under 35 USC §103(a) in view of U.S. Patent No. 6,092,202 (Veil) and "*When A Password Is Not A Password*" (Weiss)

This rejection is respectfully traversed on the grounds that the Weiss article, like the Veil patent, neither discloses nor suggests the *combination* of:

(a) a smartcard that performs all operations involving the private key so that the file signing tool is not required to retrieve the private key from the smartcard; and

(b) protection of the smartcard by multiple PINs..

Instead, the Weiss article discusses the use of security tokens and challenge response scripts to *supplement* conventional single PINs or passwords, such as the ones that Veil relies upon to protect private keys retrieved by the file signing tool (security co-processor 122). There is no suggestion in the Weiss publication of having a smartcard perform signing operations that might reveal a private key, while utilizing a file signing tool to perform the signing operation, nor is there is there a suggestion of using multiple PINs to protect access to the smartcard, as specifically recited in claim 10.

The challenge response arrangement if Weiss is clearly not the same as multiple PINs. PINs are numbers that are stored in the device for self-verification. In Weiss, a single PIN stored on the token is used to protect the token. The challenge-response protocol cited by the Examiner is not equivalent to the PIN, but rather is carried out by the controller of the terminal with which the token is to be used. As explained in the paragraph bridging pages 107-108 of the Weiss publication, entry of a single correct PIN provides access to a device. The challenge response routine does not even begin until after verification of the PIN, and involves encryption of the user's response ***by the token*** (*i.e.*, the smartcard), access to the encryption device having been granted upon entry of the PIN. **The challenge-response routine verifies the token, rather than protecting access to the token**. Thus, neither the password nor the challenge-response disclosed by Weiss can be considered equivalent to multiple smartcard-protecting PINs, as claimed.

Since the Weiss publication does not disclose the multiple PINs of claim 10, withdrawal of the rejection of claim 10 under 35 USC §103(a) is respectfully requested.

4. Rejection of Claim 20 Under 35 USC §103(a) in view of U.S. Patent Nos. 6,092,202 (Veil) and 5,7521,781 (Deo), and "*When A Password Is Not A Password*" (Weiss)

This rejection is respectfully traversed on the grounds that the Deo patent, like the Weiss article and the Veil patent, neither discloses nor suggests a file signing tool, as claimed, that is arranged to perform the functions of receiving a file to be signed; signing the file by accessing a smartcard *without retrieving a private key from the smartcard*, and downloading the signed file to a terminal. Furthermore, the Deo patent, like the Veil patent and Weiss article, does not disclose the claimed requirement that multiple PINs be entered before access to the smartcard is granted.

Instead, the Deo patent discloses a system in which a smartcard is inserted into a terminal and exchanges certificates with a terminal to provide mutual authentication, with different PINs and certificates assigned to different applications. There is no suggestion of the terminal accessing the smartcard in order to sign a file for download to another terminal, and therefore the terminal of Deo cannot be considered to correspond to the claimed **file signing tool**. Furthermore, there is no suggestion of the claimed **multiple PINs** for accessing the smartcard. Instead, Deo discloses that different PINs are used to protect different applications on the smartcard. In the system of Deo, to access any particular application on the smartcard, **only a single PIN need be entered**. ***Requiring entry of different PINs to access different applications is not the same as requiring entry of multiple PINs before any access to the smartcard is granted.***

Withdrawal of the rejection of claim 20 under 35 USC §103(a) is accordingly respectfully requested.

Serial Number 09/893,465

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: July 12, 2005

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500